ITU Regional Cybersecurity Forum for Asia-Pacific

- Connecting the World Responsibly -

Hyderabad, India
23-25 September 2009

Working Together to Ensure Cybersecurity in the Asia-Pacific Region

In concluding the **ITU Regional Cybersecurity Forum for Asia-Pacific**, the participants agreed on the following outcomes:

- Acknowledged the usefulness of the Regional Cybersecurity Forum as a platform for representatives from government and private sector, international organizations and academia to come together to discuss and elaborate on concrete steps to build cybersecurity capacity and competency in the region.
- Recognized that cybersecurity is a global issue that requires cooperation across national borders. As such, measures at the national as well as global levels are required to deal with the various aspects of cyber-threats to ensure the safety and security of critical infrastructures in countries. Recognized the usefulness of the ITU Global Cybersecurity Agenda (GCA) as a mechanism and framework for international cooperation for cybersecurity. The delegates encouraged countries to undertake activities that relate to the five work areas of the GCA: 1. Legal Measures; 2. Technical and Procedural Measures; 3. Organizational Structures, 4. Capacity Building, and 5. International Cooperation, and share their experiences in implementing these initiatives on the national level with other countries in the region.
- Emphasized that cybersecurity is increasingly important for countries in the Asia-Pacific region, and governments need to be well informed and coordinated on this topic. With the evolution of technologies, the nature of cyber-threats and the overall threat landscape is constantly changing. Governments must be aware of these changes and take the necessary measures at the national level.
- Acknowledged that a coordinated national response requires the participation of all relevant stakeholders and includes awareness and engagement at all levels. All different stakeholders have a role to play and government leadership in coordinating the national response is critical.
- Noted that the level of preparedness in responding to cyber-threats is very different in the countries in the region.
- Encouraged countries in the region to actively share information and experiences, good practices and explore partnership opportunities for effective cybersecurity responses. Highlighting the need to build these partnerships on mutual trust and ensure a win-win approach based on a demonstrable and measurable value proposition. Only by working together to elaborate strategies, identifying best practices, and implementing concrete solutions, can the global challenges be addressed.
- Encouraged countries to incorporate initiatives on how to protect children online in their national cybersecurity efforts, and contribute to regional and global activities and initiatives, such as the ITU's Child Online Protection (COP) initiative. With a pervasive ICT uptake in societies today and in particular among young generations, children and youth are very vulnerable to harms in cyber space. Issues such as child pornography, access to

inappropriate content, child abuse images, online harassments and etc. need to be urgently addressed and enhanced cooperation is required in this regard.

- Noted that a baseline level of cybersecurity awareness is required among the population at large in order to move forward toward building a user centric and development oriented information society.
- Highlighted the need for capacity building across all different areas of cybersecurity. Noting that this is relevant for developing and developed countries alike as scarce resources, expert skills, and capacity are lacking in most countries. It is important to know what base-line skills and capacity need to be built. A good starting point is documenting existing capabilities, identifying gaps and requirements, and based on this develop specific capacity development programs for countries and communities in the Asia-Pacific region.
- Noted that conducting a national cybersecurity self-assessment using existing tools and material such as the ITU National Cybersecurity/CIIP Self-Assessment Tool can be useful for countries to help identify where the different national parties are at with regards to cybersecurity readiness and preparedness, what they are doing, what they could do next and as a result identify practical steps forward on developing a national cybersecurity strategy. The Tool is a practical instrument that can assist national authorities to: understand and review their domestic situation, identify and prioritize areas for attention, and lay out a plan of action.
- Committed to take action on **developing a national cybersecurity strategy** and ensure that international cooperation is taken into consideration in the development of the different national cybersecurity building blocks.
- Noted the need to share information and best practices amongst the countries in the area of **developing a legal framework and establishing effective enforcement.** Existing resources and tools like the ITU Understanding Cybercrime Guide and Toolkit for Cybercrime Legislation were mentioned as useful resources in this regard. As ICTs evolve rapidly, legislation and regulation that deal with cybercrime and criminalizing the misuse of ICTs require continuous review and revision.
- Expressed the need to share information and assist one and other in **developing national watch and warning and incident management capabilities** and noted that in order to facilitate the development of cybersecurity capabilities, including the establishment of national CIRTs, the resources and services made available by the ITU in collaboration with key partners, such as the International Multilateral Partnership Against Cyber Threats (IMPACT), governments and other stakeholders in the region such as existing CERTs, is useful.
- Acknowledged the services provided to countries through the ITU-IMPACT collaboration allow countries to prepare themselves against cyber threats, and ensure at the same time coordination and cooperation at the national and international levels. In this regard ITU encouraged those administrations in the region that have not yet joined the ITU-IMPACT alliance, to consider joining.
- Acknowledged the usefulness of the dedicated training provided at the Forum on three main topics: developing a national cybersecurity strategy; building national watch, warning and incident response capabilities; and, drafting and reviewing legislation to criminalize the misuse of ICTs.

More details on the ITU Regional Cybersecurity Forum for Asia-Pacific can be found on the event website at: www.itu.int/ITU-D/cyb/events/2009/hyderabad/